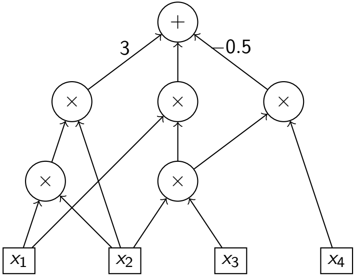
Hitting Sets for *UPT* Circuits

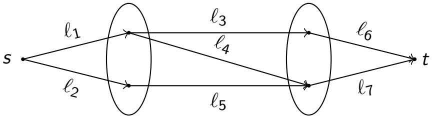
Ramprasad Saptharishi and Anamay Tengse

TIFR, Mumbai, India

6th March 2018

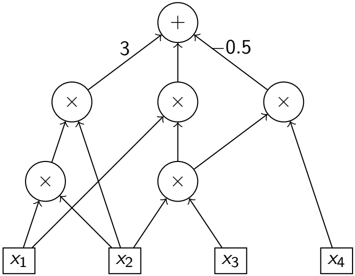
Non-commutative models

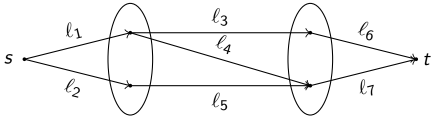




- $x_1 x_2 x_1 \neq x_1 x_1 x_2$
  monomials $\sim$ words
- Introduced by Nisan [N91]
- Circuits:
  No. of nodes
- ABPs:
  Width, No. of layers

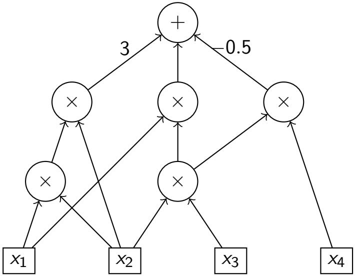
Non-commutative models

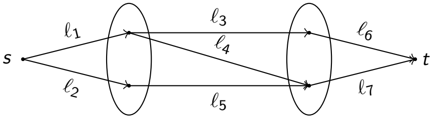




- $x_1x_2x_1 \neq x_1x_1x_2$
  monomials $\sim$ words
- Introduced by Nisan [N91]
- Circuits:
  No. of nodes
- ABPs:
  Width, No. of layers
- ABPs $\subsetneq$ Circuits
  [N91]

Non-commutative models





- $x_1x_2x_1 \neq x_1x_1x_2$
  monomials $\sim$ words
- Introduced by Nisan [N91]
- Circuits:
  No. of nodes
- ABPs:
  Width, No. of layers
- ABPs $\subsetneq$ Circuits
  [N91]

Homogeneous circuits: Each gate is homogeneous
Homogeneous ABPs: Each of the ℓ_is are homogeneous

Hitting sets for Non-commutative circuits

Given a non-commutative circuit class $\mathcal{C} \subseteq \mathbb{F}\langle \mathbf{x} \rangle$, a set of *matrices* $\mathcal{H}$ is called a hitting set for $\mathcal{C}$ if a nonzero $C \in \mathcal{C}$ evaluates to a nonzero value on at least one input from $\mathcal{H}$.

Note: Variables from $\mathbf{x}$ can be thought of as matrices with commuting variables from $\mathbf{y}$ as entries.

Strategy: Substitute univariates of low degree, interpolate.

$$\phi : \mathbf{y} \to \mathbb{F}[t].$$

Hitting sets for Non-commutative circuits

Given a non-commutative circuit class $\mathcal{C} \subseteq \mathbb{F}\langle \mathbf{x} \rangle$, a set of *matrices* $\mathcal{H}$ is called a hitting set for $\mathcal{C}$ if a nonzero $C \in \mathcal{C}$ evaluates to a nonzero value on at least one input from $\mathcal{H}$.

Note: Variables from $\mathbf{x}$ can be thought of as matrices with commuting variables from $\mathbf{y}$ as entries.

Strategy: Substitute univariates of low degree, interpolate.

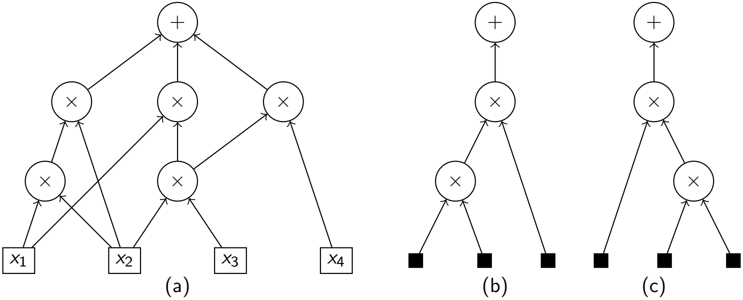
$$\phi : \mathbf{y} \to \mathbb{F}[t].$$

For this talk:

- Non-commutative circuits, ABPs
- WLOG models will be homogeneous

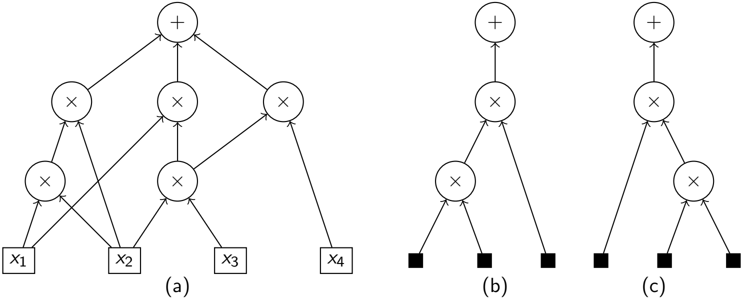
Parse Trees and Unambiguity

Parse tree: Start from root, one child of $+$, all children of $\times$



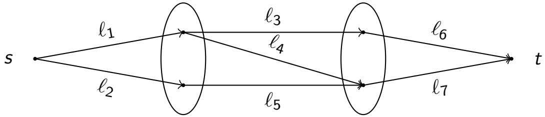
Parse Trees and Unambiguity

Parse tree: Start from root, one child of $+$, all children of $\times$

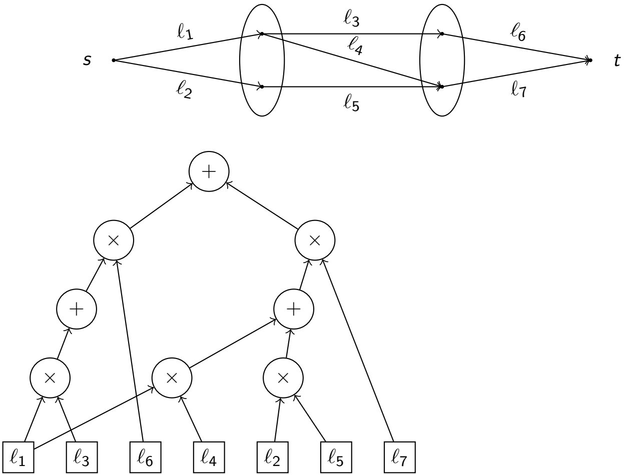


- Unambiguous or Unique Parse Tree (UPT) [LMP16]
  all parse trees have the same shape.
- ABPs $\subsetneq$ UPT $\subsetneq$ Circuits [LMP16]

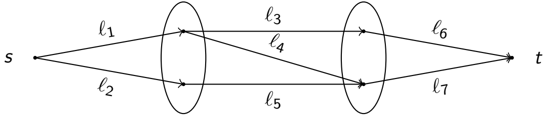
ABPs as UPT circuits

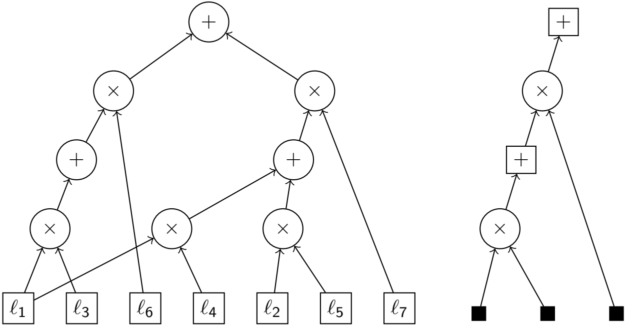


ABPs as UPT circuits

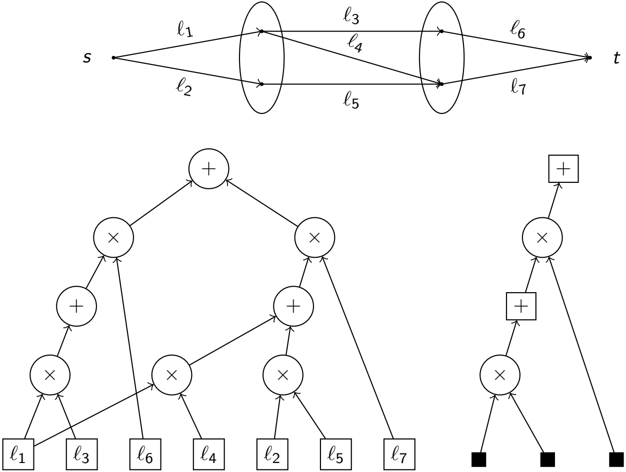


ABPs as UPT circuits





ABPs as UPT circuits



- ABPs are UPT circuits with *left-skew* tree.

Properties of UPT circuits [LMP16]

1. WLOG each gate appears in a fixed position in the tree.
   Can be done with a d blow-up.
2. Natural notion of *width* of a position.
   No. of gates appearing in that position.
   Analogous to width of an ABP.
3. All product gates are *position disjoint*.
   Consequence of 1.
   Similar to edges in different layer segments in an ABP.

Properties of UPT circuits [LMP16]

1. WLOG each gate appears in a fixed position in the tree.
   Can be done with a d blow-up.
2. Natural notion of *width* of a position.
   No. of gates appearing in that position.
   Analogous to width of an ABP.
3. All product gates are *position disjoint*.
   Consequence of 1.
   Similar to edges in different layer segments in an ABP.

Plan:

- Overview of hitting sets for ABPs.
- Extend ideas to UPT circuits.

Quick survey

- Nisan's characterization for ABPs [N91].

Quick survey

- Nisan's characterization for ABPs [N91].
- [RS05] gave *White box* PIT for ABPs in poly(n).

Quick survey

- Nisan's characterization for ABPs [N91].
- [RS05] gave *White box* PIT for ABPs in poly(n).
- [FS13] *Known order* hitting sets for ROABPs in $n^{O(\log n)}$.

Quick survey

- Nisan's characterization for ABPs [N91].
- [RS05] gave *White box* PIT for ABPs in poly(n).
- [FS13] *Known order* hitting sets for ROABPs in $n^{O(\log n)}$.
- [AGKS15] *Unknown order* hitting sets for ROABPs in $n^{O(\log n)}$.
  Basis Isolating Weight Assignment (BIWA).

Quick survey

- Nisan's characterization for ABPs [N91].
- [RS05] gave *White box* PIT for ABPs in poly(n).
- [FS13] *Known order* hitting sets for ROABPs in $n^{O(\log n)}$.
- [AGKS15] *Unknown order* hitting sets for ROABPs in $n^{O(\log n)}$.
  Basis Isolating Weight Assignment (BIWA).
- Hitting sets for models related to ROABPs
  - Constant width, known order in poly(n) [GKS16].
  - Sum of c ROABPs: *white box* in poly(n), hitting sets $n^{O(\log n)}$ [GKST15] (Nisan's characterization + BIWA).

Quick survey

- Nisan's characterization for ABPs [N91].
- [RS05] gave *White box* PIT for ABPs in poly(n).
- [FS13] *Known order* hitting sets for ROABPs in $n^{O(\log n)}$.
- [AGKS15] *Unknown order* hitting sets for ROABPs in $n^{O(\log n)}$.
  Basis Isolating Weight Assignment (BIWA).
- Hitting sets for models related to ROABPs
  - Constant width, known order in poly(n) [GKS16].
  - Sum of c ROABPs: *white box* in poly(n), hitting sets $n^{O(\log n)}$ [GKST15] (Nisan's characterization + BIWA).
- [LMP16] introduced UPT circuits
  - Extend Nisan's characterization
  - *White box* in poly(n)

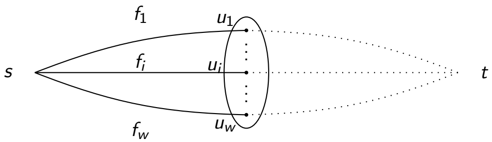
Quick survey

- Nisan's characterization for ABPs [N91].
- [RS05] gave *White box* PIT for ABPs in poly(n).
- [FS13] *Known order* hitting sets for ROABPs in $n^{O(\log n)}$.
- [AGKS15] *Unknown order* hitting sets for ROABPs in $n^{O(\log n)}$.
  Basis Isolating Weight Assignment (BIWA).
- Hitting sets for models related to ROABPs
  - Constant width, known order in poly(n) [GKS16].
  - Sum of c ROABPs: *white box* in poly(n), hitting sets $n^{O(\log n)}$ [GKST15] (Nisan's characterization + BIWA).
- [LMP16] introduced UPT circuits
  - Extend Nisan's characterization
  - *White box* in poly(n)
- [LLS17] extend *white box* results of [GKST15].

Quick survey

- Nisan's characterization for ABPs [N91].
- [RS05] gave *White box* PIT for ABPs in poly(n).
- [FS13] *Known order* hitting sets for ROABPs in $n^{O(\log n)}$.
- [AGKS15] *Unknown order* hitting sets for ROABPs in $n^{O(\log n)}$.
  Basis Isolating Weight Assignment (BIWA).
- Hitting sets for models related to ROABPs
  - Constant width, known order in poly(n) [GKS16].
  - Sum of c ROABPs: *white box* in poly(n), hitting sets $n^{O(\log n)}$ [GKST15] (Nisan's characterization + BIWA).
- [LMP16] introduced UPT circuits
  - Extend Nisan's characterization
  - *White box* in poly(n)
- [LLS17] extend *white box* results of [GKST15].
- *This work*: BIWA for UPT circuits, extends hitting sets of [AGKS15,GKST15,GKS15].

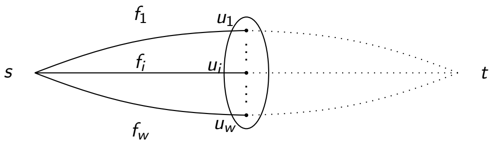
Coefficient span [RS05,FS13]



Preserve nonzeroness of an arbitrary linear combination of f_is.

$$M_f = \begin{bmatrix} \leftarrow & f_1 & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & f_w & \rightarrow \end{bmatrix} \in \mathbb{F}[\mathbf{y}]^k \equiv \mathbb{F}^k[\mathbf{y}]$$

Coefficient span [RS05,FS13]



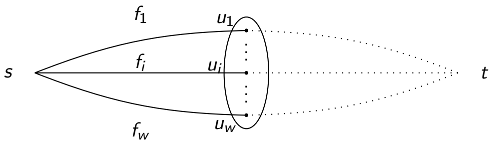
Preserve nonzeroness of an arbitrary linear combination of f_is.

$$M_f = \begin{bmatrix} \leftarrow & f_1 & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & f_w & \rightarrow \end{bmatrix} \in \mathbb{F}[\mathbf{y}]^k \equiv \mathbb{F}^k[\mathbf{y}]$$

Consider $\phi : \mathbf{y} \to \mathbb{F}[t_1, \ldots, t_k]$ $\qquad (k \sim \log n)$

Such a ϕ sends columns of M_f to $n^{O(k)}$ columns.

Coefficient span [RS05,FS13]



Preserve nonzeroness of an arbitrary linear combination of f_is.

$$M_f = \begin{bmatrix} \leftarrow & f_1 & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & f_w & \rightarrow \end{bmatrix} \in \mathbb{F}[\mathbf{y}]^k \equiv \mathbb{F}^k[\mathbf{y}]$$

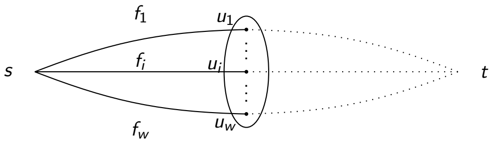
Consider $\phi : \mathbf{y} \to \mathbb{F}[t_1, \ldots, t_k]$ $(k \sim \log n)$

Such a ϕ sends columns of M_f to $n^{O(k)}$ columns.

[FS13] A ϕ that preserves colSpan(M_f) suffices.

ColSpan(M_f) = CoeffSpan$(f_1, \ldots, f_w)$

Coefficient span [RS05,FS13]



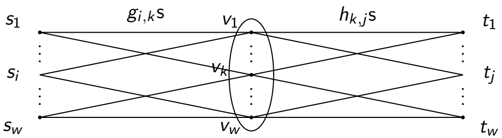
[FS13] A ϕ that preserves colSpan(M_f) suffices.

Let $(wt_1, \ldots, wt_k) : \mathbf{y} \to [N]^k$ and ϕ_{wt} be such that $\phi_{wt} : y_i \mapsto t_1^{wt_1(y_i)} \cdots t_k^{wt_k(y_i)}$.

[AGKS15] If *wt* is a basis isolating weight assignment (BIWA) for M_f, then ϕ_{wt} will preserve CoeffSpan.

How do we construct a BIWA?

Basis Isolation [AGKS15]

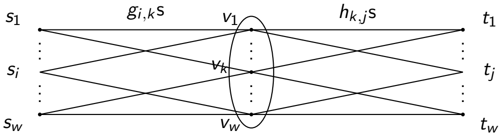


$$M_f \qquad M_g \qquad M_h$$

$$\begin{bmatrix} \leftarrow & f_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & f_{w,w} & \rightarrow \end{bmatrix} \quad \begin{bmatrix} \leftarrow & g_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & g_{w,w} & \rightarrow \end{bmatrix} \quad \begin{bmatrix} \leftarrow & h_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & h_{w,w} & \rightarrow \end{bmatrix}$$

Define V_f, V_g, V_h, where $V_* = \text{rowSpan}(M_*)$.

Basis Isolation [AGKS15]



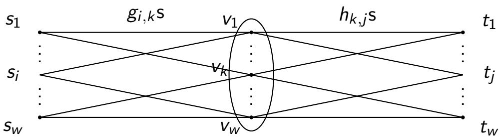
$$M_f \qquad M_g \qquad M_h$$

$$\begin{bmatrix} \leftarrow & f_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & f_{w,w} & \rightarrow \end{bmatrix} \quad \begin{bmatrix} \leftarrow & g_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & g_{w,w} & \rightarrow \end{bmatrix} \quad \begin{bmatrix} \leftarrow & h_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & h_{w,w} & \rightarrow \end{bmatrix}$$

Define V_f, V_g, V_h, where $V_* = \text{rowSpan}(M_*)$.

$$f_{i,j} = \sum_{k \in [w]} g_{i,k} h_{k,j} \qquad \in V_f \subseteq V_g \otimes V_h$$

Basis Isolation [AGKS15]



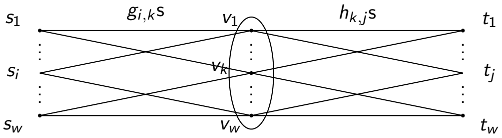
$$M_f \qquad\qquad M_g \qquad\qquad M_h$$

$$\begin{bmatrix} \leftarrow & f_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & f_{w,w} & \rightarrow \end{bmatrix} \qquad \begin{bmatrix} \leftarrow & g_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & g_{w,w} & \rightarrow \end{bmatrix} \qquad \begin{bmatrix} \leftarrow & h_{1,1} & \rightarrow \\ \leftarrow & \vdots & \rightarrow \\ \leftarrow & h_{w,w} & \rightarrow \end{bmatrix}$$

Define V_f, V_g, V_h, where $V_* = \text{rowSpan}(M_*)$.

$$f_{i,j} = \sum_{k \in [w]} g_{i,k} h_{k,j} \qquad \in V_f \subseteq V_g \otimes V_h$$

Basis Isolation [AGKS15]



Define V_f, V_g, V_h, where $V_* = \text{rowSpan}(M_*)$.

$$f_{i,j} = \sum_{k \in [w]} g_{i,k} h_{k,j} \qquad \in V_f \subseteq V_g \otimes V_h$$

BIWA [AGKS15]:

If $\mathbf{wt} : \mathbf{y} \to [N]^k$ is a BIWA for V_g and V_h, then poly(n) time construction for $wt' : \mathbf{y} \to [N]$ such that $(\mathbf{wt}, wt') : \mathbf{y} \to [N]^{k+1}$ is a BIWA for V_f.

So far...

Abstract view of [AGKS15]

- Each layer segment with w^2 edges naturally yields a vector space.
- Space V_f resulting from paths across consecutive layers (V_g, V_h) satisfies $V_f \subseteq V_g \otimes V_h$.
- BIWA for V_g and V_h can be extended to a BIWA for V_f by adding an extra coordinate, in poly(n) time.

So far...

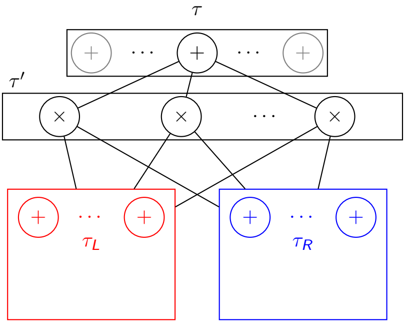
Abstract view of [AGKS15]

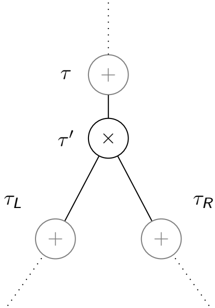
- Each layer segment with w^2 edges naturally yields a vector space.
- Space V_f resulting from paths across consecutive layers (V_g, V_h) satisfies $V_f \subseteq V_g \otimes V_h$.
- BIWA for V_g and V_h can be extended to a BIWA for V_f by adding an extra coordinate, in poly(n) time.

Properties of UPT circuits

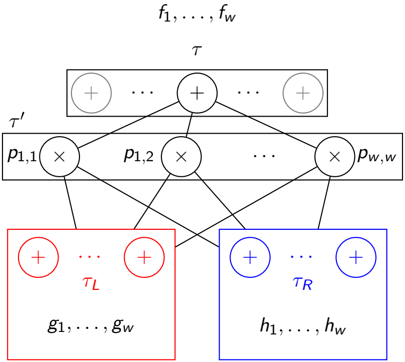
- All parse trees have the same shape, each gate $\sim$ node.
- Analogous notion of *width* for nodes.
- All product gates are position disjoint.

Extending AGKS to UPT ckts



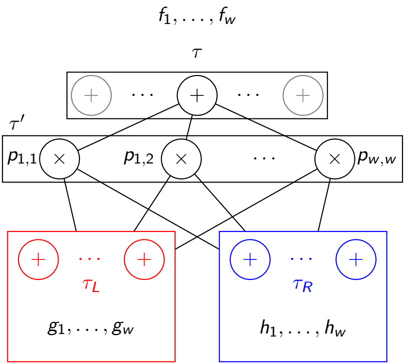


Extending AGKS to UPT ckts



$$p_{i,j} = g_i \times h_j$$
$$f_k \in \langle \{g_i \times h_j : (i,j) \in [w]^2\} \rangle$$

Extending AGKS to UPT ckts



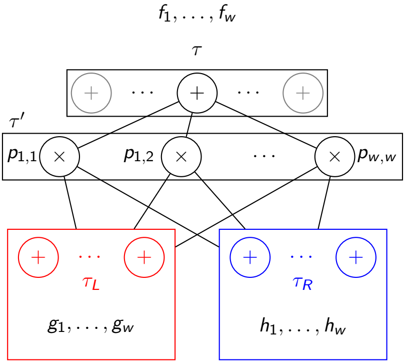
$p_{i,j} = g_i \times h_j$

$f_k \in \langle \{ g_i \times h_j : (i,j) \in [w]^2 \} \rangle$

$$V_\tau \equiv \begin{bmatrix} \leftarrow & f_1 & \rightarrow \\ & \vdots & \\ \leftarrow & f_w & \rightarrow \end{bmatrix}$$

$V_{\tau'}, V_{\tau_L}, V_{\tau_R}$.

Extending AGKS to UPT ckts



$$p_{i,j} = g_i \times h_j$$
$$f_k \in \langle \{g_i \times h_j : (i,j) \in [w]^2\} \rangle$$

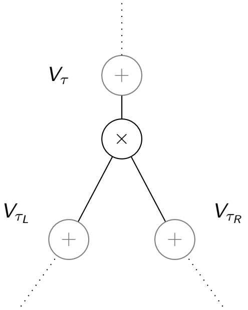
$$V_\tau \equiv \begin{bmatrix} \leftarrow & f_1 & \rightarrow \\ & \vdots & \\ \leftarrow & f_w & \rightarrow \end{bmatrix}$$

$V_{\tau'}, V_{\tau_L}, V_{\tau_R}$.

$V_\tau \subseteq V_{\tau'}$ $\qquad V_{\tau'} = V_{\tau_L} \otimes V_{\tau_R}$

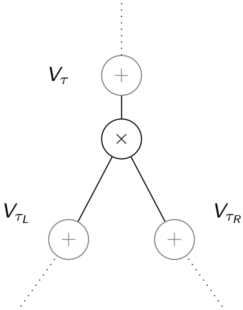
$$V_\tau \subseteq V_{\tau_L} \otimes V_{\tau_R}$$

BIWA for UPT circuits



Lemma [AGKS15]
If $(wt_1, \ldots, wt_k)$ is a BIWA for *both* V_{τ_L} and V_{τ_R}, then in poly(n) time we can find wt_{k+1} such that $(wt_1, \ldots, wt_{k+1})$ is a BIWA for all V_τ.

BIWA for UPT circuits

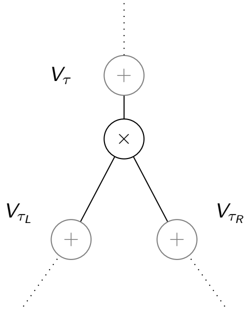


Lemma [AGKS15]

If $(wt_1, \ldots, wt_k)$ is a BIWA for *both* V_{τ_L} and V_{τ_R}, then in poly(n) time we can find wt_{k+1} such that $(wt_1, \ldots, wt_{k+1})$ is a BIWA for all V_τ.

BIWA for V_{root} with at most as many coordinates as depth(C).

BIWA for UPT circuits



Lemma [AGKS15]

If $(wt_1, \ldots, wt_k)$ is a BIWA for *both* V_{τ_L} and V_{τ_R}, then in poly(n) time we can find wt_{k+1} such that $(wt_1, \ldots, wt_{k+1})$ is a BIWA for all V_τ.

BIWA for V_{root} with at most as many coordinates as depth(C).

Depth Reduction by *shuffling*

For every UPT $\mathbf{C}$ of degree d, an *equivalent* UPT $\sigma(\mathbf{C})$ of depth $O(\log d)$ exists.

Concluding remarks

Not covered:

- Extending hitting sets for sum of c ROABPs [GKST15] and constant *width* ROABPs [GKS16] to UPT circuits.
- Exponential lower bound against UPT circuits under *shufflings* for the *moving pallindrome* defined in [LMP16].
- Quasipolynomial (tight) separation between ABPs and UPT circuits under *shufflings*, extension of [HY16].

Concluding remarks

Not covered:

- Extending hitting sets for sum of c ROABPs [GKST15] and constant *width* ROABPs [GKS16] to UPT circuits.
- Exponential lower bound against UPT circuits under *shufflings* for the *moving pallindrome* defined in [LMP16].
- Quasipolynomial (tight) separation between ABPs and UPT circuits under *shufflings*, extension of [HY16].

Question: ABPs are UPT circuits with *skew* trees. Can we construct hitting sets for *skew circuits*?

Concluding remarks

Not covered:

- Extending hitting sets for sum of c ROABPs [GKST15] and constant *width* ROABPs [GKS16] to UPT circuits.
- Exponential lower bound against UPT circuits under *shufflings* for the *moving pallindrome* defined in [LMP16].
- Quasipolynomial (tight) separation between ABPs and UPT circuits under *shufflings*, extension of [HY16].

Question: ABPs are UPT circuits with *skew* trees. Can we construct hitting sets for *skew circuits*?

Thank you.